SharkFest '18 Europe

Crash Course: IPv6 & Network Protocols

by looking at packets!

Johannes Weber

Network Security Consultant

#whoami: Johannes Weber

- Network Security Consultant
  @ TÜV Rheinland i-sec GmbH
  - (Next-Gen) Firewalls
  - VPN/Crypto
  - Routing/Switching
- IPv6, DNS, NTP
- https://weberblog.net
- @webernetz

Agenda/Motivation

- Many „unknown“ packets
  - IPv6
  - Network Protocols
- Crash course -> fast, no deep dive & skipping ;)
- Normally: 2 day workshop for IPv6 only
- Never ending acronyms

- Who is familiar with IPv6?

Tracefiles

- https://tinyurl.com/ipv6-crash-course
- -> download of „weber01.zip“
- -> 3x pcaps
- Plz do me a favour: listen first ;)
- flavoured with 12x challenges

IPv6

- IPv4 space is exhausted
- IPv6 brings enough addresses ;)
  - every client is global addressable
  - end-to-end communication (no NAT!)
  - subnets for everyone
- Only layer 3 changes (almost)
- No broadcast anymore, but multicast

IPv6 Addresses

- 128 bits long, hexadecimal, 8 groups called „hextets“
- Notation: address/prefix-length
- Address abbreviation
  - `2001:0db8:0000:0000:cafe:0000:1200:f1b2`
  - `2001:db8::cafe:0:1200:f1b2`
- Subnets ALWAYS /64

IPv6 Addresses

- Unspecified `::`
- Link-Local, LL `fe80::`
- Multicast `ff00::/8`, mostly `ff02::`

- Every (!) node gets one link-local
  AND couple of global unicast addresses, GUA

IPv6 Address Assignment

- Manual, stateful DHCPv6
- SLAAC through router advertisement, RA
  - Router sends RA with /64 prefix
  - Client generates interface-ID, IID
  - Client sends duplicate address detection, DAD through neighbor solicitation, NS
  - Recursive DNS server through RA or stateless DHCPv6

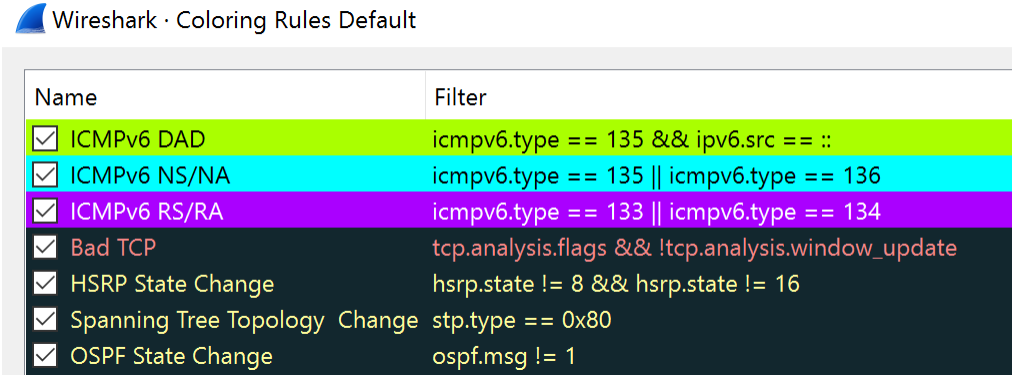
IPv6 Address Assignment

- IIDs normally through EUI-64, i.e., MAC address
  `::ca0e:14ff:fe7e:339f`
- or stable opaque
  `::263d:a07f:df5:bcfb`
- and/or temporary (privacy extension, PE)

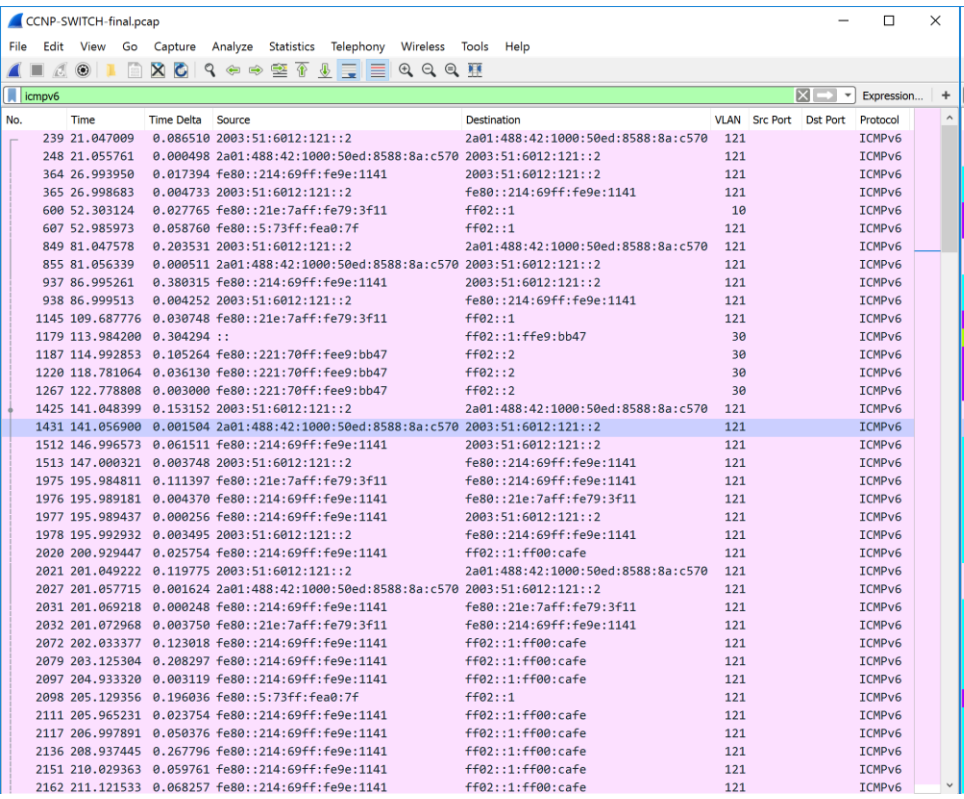
IPv6 Address Assignment

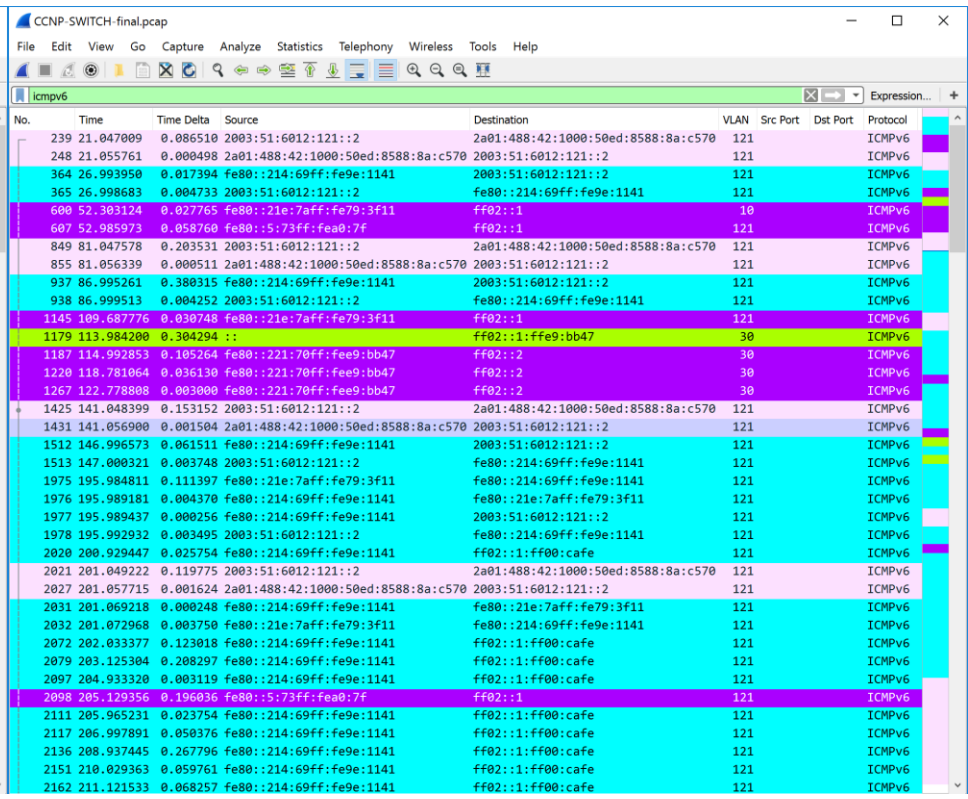
- Problem: Everything is within ICMPv6
- Suite called Neihbor Discovery Protocol, NDP
  - Router Solicit./Advert.: `icmpv6.type == 133/134`
  - Neighbor Solicit./Advert.: `icmpv6.type == 135/136`
- DHCPv6: `dhcpv6`
- Use Coloring Rules for RS/RA, NS/NA, DAD

IPv6 Address Assignment



IPv6 Address Assignment





IPv6 Address Assignment

- → Wireshark time… 1st pcap
- RS/RA: message 8, 12
- DAD: message 21
- DHCPv6: message 13 & 14 (recursive DNS)

- Challenge: Flags from the prefix information?
  - On-link (L), Autonomous address-configuration (A)

Link-Layer Addr. Resolution

- ARP in IPv4
- Neighbor solicitation sent to special multicast addresses … ;(
  - `2003:50:aa10:4243:221:6aff:fe2d:3b8e`
  - `ff02::1:ff2d:3b8e`
- Target answers wich neighbor advertisement
- `icmpv6.type == 135 or icmpv6.type == 136`

IPv6 Address Assignment

- → Wireshark time… 1st pcap
- NS: message 53 w/ link-layer option!
- NA: message 54

What's missing?

- Annoying multicast listener stuff, MLD
- Problem again: Everything is within ICMPv6

```
icmpv6.type == 130 or icmpv6.type == 131 or
icmpv6.type == 132 or icmpv6.type == 143
```

- Filter it out ;)

```
!()
```

To sum it up

- ICMPv6 with NDP collection
  - RS/RA 133/134
  - NS/NA 135/136
  - DAD 135 from ::
  - Ping 128/129
  - Ignoring MLD
- DHCPv6

Upper Layers stay the same

- → Wireshark time… 2nd pcap
- DNS, HTTP(S), IMAP, SMTP
- SSH, SNMP, Ping
- TL;DR: Nothing to see here

- Challenge: What‘s inside the HTTP answer?
  - A table (Hint: „Follow HTTP Stream“)

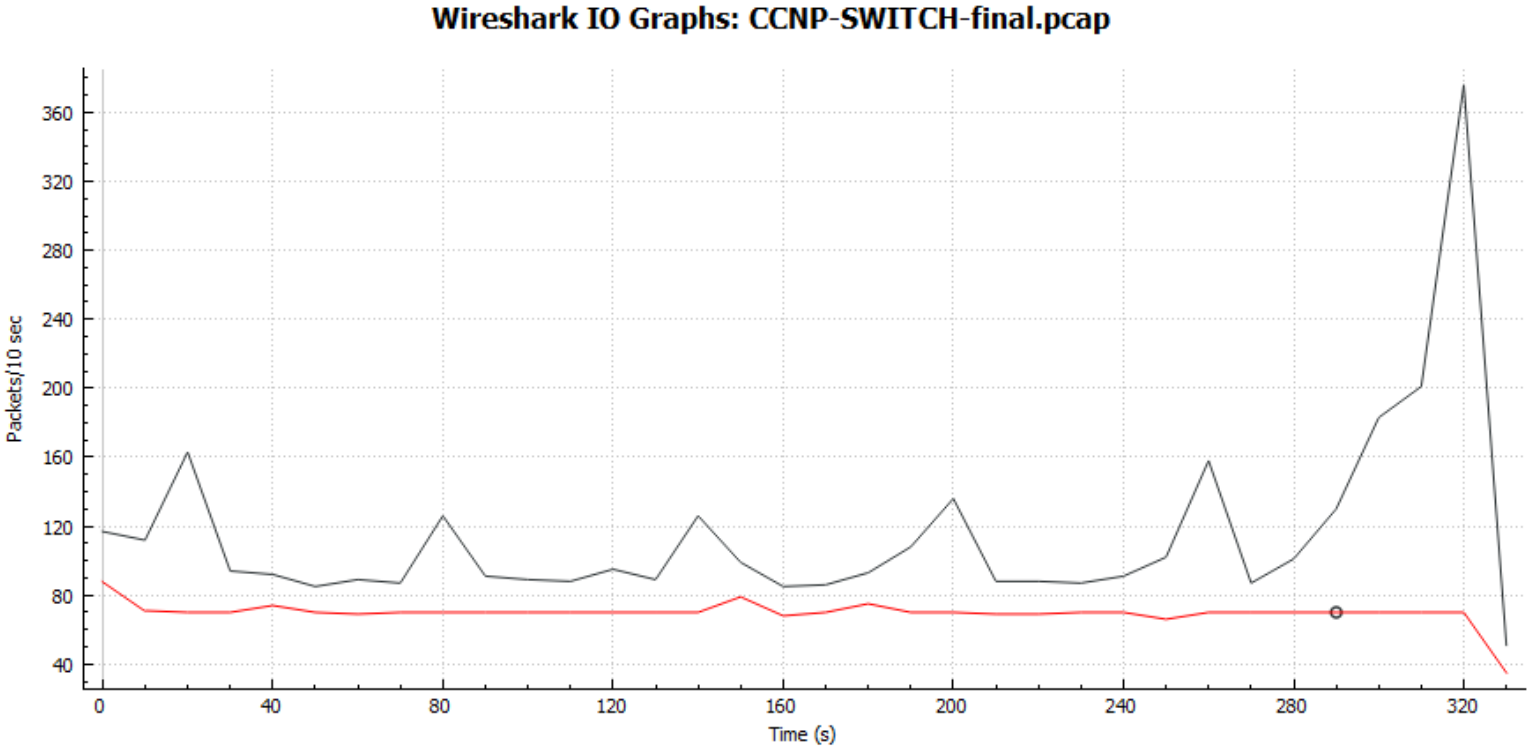
Network Protocols

- Protocols to manage switches & routers
- 5x link layer protocols (above Ethernet but not IP)
- 5x based on UDP
- `not (dns or http or smtp)`
- `not (rip or ospf or bgp)`
- → Wireshark time… 3rd pcap

Spanning Tree Protocol

- Display Filter: `stp`
- Prevents loops within switched networks
- per VLAN, today‘s default: Rapid STP
- Root bridge (= switch): central point
- Hello: every 2 seconds per port per VLAN!

Spanning Tree Protocol



Spanning Tree Protocol

- Do NOT disable it on user ports!
- Keywords: MST, BDPU, root port, designated port, port states: blocking/discarding, learning, portfast, BPDU guard, BPDU filter
- No need for STP in SDN anymore
- Challenge: Root bridge ID for VLAN 40?
  - Bridge Identifier: 24576 / 40 / 00:21:1b:ae:31:80

Cisco Discovery Protocol

- Display Filter: `cdp`
- Cisco proprietary
- Shares information about *directly connected* devices
- Keywords: TLV, CDP spoofing ;)
- Challenge: IPv4 management address of CCNP-LAB-S1?
  - 192.168.121.10

Link Layer Discovery Protocol

- Display Filter: `lldp`
- Vendor-neutral version for sharing layer 2 neighbor information
- Keywords: Information gathering ;)
- Challenge: IPv6 management address of CCNP-LAB-S1?
  - 2003:51:6012:121::10

VLAN Trunking Protocol

- Display Filter: `vtp`
- Cisco proprietary, propagates VLAN definitions (ID & name, …)
- Three different versions, recommended: v3, reality: v2
- Keywords: configuration revision number, VTP domain name, VTP password, VTP pruning
- Challenge: Name of VLAN 10? Hint: „ISL VLAN ID“ field is hexadecimal
  - VLAN10undsonstnix

Link Aggregation Control P.

- Display Filter: `lacp`
- Negotiates an automatic bundling of links
- aka Etherchannel, trunk, aggregated link group
- slow = 30s, fast = 1s
- Keywords: mode active/passive, system/port priority
- Challenge: seen from actor 00:0a:8a:a1:5a:80: what‘s the partner port priority?
  - 32768

Hot Standby Router Protocol

- Display Filter: `hsrp`
- Cisco proprietary, redundancy of the default gateway
- Hightest priority: virtual router w/ virtual IP, VIP
- Not an HA-pair of hardware, only VIPs
- Standards-based alternative: VRRP
- Keywords: HSRP group, multicast groups, virtual MAC
- Challenge: virtual IPv6 address for HSRP group 127?
  - fe80::5:73ff:fea0:7f

Syslog

- Display Filter: `syslog`
- Message logging to central server, e.g. SIEM, Splunk
- UDP port 514, plaintext
- TCP and TLS recommended
- Keywords: facility, severity level (0-7)
- Challenge: Which inteface changed state to up?
  - Interface GigabitEthernet0/2, changed state to up

Network Time Protocol

- Display Filter: `ntp`
- Clock synchronization
- UDP port 123
- Stratum 1: synced to external source (GPS, DCF77)
- Recommended: Authentication via SHA-1
- Keywords: NTP algorithm, timestamps, SNTP, PTP
- Challenge: Reference ID from IPv6 NTP server?
  - DCFa (amplitude modulation)

Simple Network Management

- Display Filter: `snmp`
- Get/set variables from management station
- Mostly: interface and CPU/memory stats
- UDP port 161, Trap on port 162, SNMPv2c plaintext!!!
- Recommended: SNMPv3 w/ encryption & authentication
- Keywords: NMS, MIB, OID, PDU
- Challenge: What‘s the used community string?
  - n5rAD1ig314IqfioYBWw

Trivial File Transfer Protocol

- Display Filter: `tftp`
- TRIVIAL file transfer, no authentication, plaintext!!
- UDP port 69
- Common usage: config files backup
- Recommended: Don‘t use it at all
- Keywords: Information gathering ;)
- Challenge: Hashed password of user weberjoh?
  - username weberjoh […] 1kI2F$Sz18KSQV/D/QJpbpIGpH10

(Security) Conclusion

- Use encryption/authentication!
- Avoid plaintext protocols!
- Expose your network carefully! ;D

- Take your own pcaps and have a look at them

Not covered

- PAgP, MST, DTP, UDLD, DHCP, ARP, LOOP, SSH, Telnet, RADIUS, TACACS+, EAPOL, SNMPv3, VRRP, GLBP, NetFlow, IP SLA, GRE, IKE, ESP, AH, RIP, OSPF, IS-IS, BGP, IGMP, PPP

Resources

- In general: Cisco CCNA/CCNP courses, Wikipedia, RFCs
- IPv6 Buzz podcast “Understanding And Troubleshooting IPv6 With Wireshark”
- Wireshark Layer 2-3 pcap Analysis w/ Challenges

Thx!

- Questions?
- johannes@webernetz.net

Stickers